Mailserver

SuSE 8.2 Postfix HOWTO Cyrus Spamschutz Virenscanner

Diese Anleitung basiert auf eine SuSE 8.2 Distrubtion und der Anleitung aus dem RootForum.

Mail & MTAs: Postfix aktualisieren und mit Blockern und Virenscanner versehen
Bei Suse 8.1 wird eine Postfix-Version 1.x installiert.
Diese ist aber nicht allzu frisch, außerdem fehlen eine Menge Features,
die man zur Viren und Spam-Abwehr benötigt.

Trotzdem sollte bei Euch schon das SuSE-Postfix installiert sein,
da es etwas einfacher macht und SuSEconfig Euch den Ärger mit den
Rechten und er chroot-Umgebung abnimmt.

Postfixversion 2.0.18.
postconf mail_version zeigt an welche Version Ihr benutzt.
postconf –m zeigt alles an was bei euch eincompiliert ist.

```
unix:~ # postconf -m
static
sdbm
pcre
nis
regexp
environ
proxy
ldap
btree
unix
hash
```

Zum bauen von Postfix werden folgende Pakete benötigt, die man mit yast
eigespielt werden.
cyrus-sasl
cyrus-sasl-devel
db-devel
openldap-lib
openldap2
openldap2-client
openldap2-devel
openssl
openssl-devel
pcre

```
unix:~ # ldd /usr/lib/postfix/smtpd #zeigt an welche libs benutzt werden.
```

Ladet Euch die neue Version von Postfix herunter:

unix:~ # cd /usr/local/src/
wget ftp://ftp.pca.dfn.de/pub/tools/net/postfix/official/postfix-2.0.18.tar.gz
gunzip postfix-2.0.18.tar.gz
tar xvf postfix-2.0.18.tar
cd postfix-2.0.18/

make tidy

SASL1:
[code]make makefiles CCARGS="-DHAS_LDAP -DHAS_PCRE -DUSE_SASL_AUTH -DHAS_SSL "
AUXLIBS="-lldap -llber -lpcre -lsasl -lssl -lcrypto"[/code]
SASL1+MYSQL:
make makefiles CCARGS="-DHAS_LDAP -DHAS_PCRE -DUSE_SASL_AUTH -DHAS_SSL -DHAS_MYSQL" AUXLIBS="-lldap -llber -lpcre -lsasl -lssl -lcrypto -L/usr/lib/mysql -lmysqlclient -lz -lm"

(Das ist alles in einer einzelnen Zeile zu schreiben!)
Falls Ihr mit mysql-Unterstützung arbeiten wollt, gebt das ein:

SASL2:
make makefiles CCARGS="-DHAS_LDAP -DHAS_PCRE -DUSE_SASL2_AUTH -DHAS_SSL " AUXLIBS="-lldap -llber -lpcre -lsasl2 -lssl -lcrypto"

SASL2+MYSQL:
make makefiles CCARGS="-DHAS_LDAP -DHAS_PCRE -DUSE_SASL2_AUTH -I/usr/include/sasl2 -DHAS_SSL -DHAS_MYSQL -I/usr/include/mysql" AUXLIBS="-lldap -llber -lpcre -L/usr/lib -lsasl2 -lssl -lcrypto -L/usr/lib -lmysqlclient -lz -lm"

(Auch das ist alles in einer einzelnen Zeile zu schreiben!)

[code]make[/code]

Wenn hier Fehler auftreten (meist fehlende Libs) dann behebt die durch installieren den nötigen Libs (achtet darauf, das ihr immer das *-devel-Zeug benötigt!)

[code]postconf -m[/code]

static
sdbm
pcre
nis
regexp
environ
proxy
ldap
btree
unix
hash

[code]
unix:/usr/local/src/postfix-2.0.18 # newaliases
unix:/usr/local/src/postfix-2.0.18 # rcpostfix stop
unix:/usr/local/src/postfix-2.0.18 # make upgrade
unix:/usr/local/src/postfix-2.0.18 # rcpostfix start[/code]

Jetzt öffnet mit tail –f /var/log/mail das log und schaut,
ob irgendwelche Fehler aufgetaucht sind.
Wenn nicht, toll, dann habt ihr jetzt ein neues Postfix.
Wenn Warnungen im Log aufgetreten sind, liegt das wahrscheinlich daran,
das Postfix ein paar Konfigurationen umbenannt hat.
Das ist nicht wild, sucht einfach nach der alten (wie im Log angegeben)
und ersetzt diese durch die neue (auch wie im Log angegeben).
Anschließend noch ein Restart:

[code]unix:~ # rcpostfix restart[/code]

Und wieder Logfiles kontrollieren.

Nachdem Postfix nun richtig läuft, können wir mal anfangen das ganze
zu konfigurieren und unsere User vor Viren, Spam und (eigener?) Dummheit
schützen.

unix:~ # cd /etc/postfix/
unix:/etc/postfix/ # wget http://www.twosteps.net/download/checks.tgz
unix:/etc/postfix/ # tar xvzf checks.tgz

Das holt die Body/Mime und Header-Check-Dateien von einem meiner Server
und entpackt diese unter dem Postfix-Verzeichnis.

Nun müssen wir die main.cf noch anpassen:

unix:/etc/postfix/ # mcedit main.cf

Fügt dort folgendes ziemlich weit unten ein:

header_checks = pcre:/etc/postfix/header_checks
body_checks = pcre:/etc/postfix/body_checks
mime_header_checks = regexp:/etc/postfix/mime_header_checks

Unter strict_rfc821_envelopes tragt Ihr die Spamlists ein,
die euch gefallen. Mit gefallen spamhaus, ordb und dsbl, aber jeder wie er es mag ;)

maps_rbl_domains = sbl.spamhaus.org,
relays.ordb.org,
unconfirmed.dsbl.org

Euere smtpd_recipient_restrictions sollte in etwa so aussehen:
(achtet auf die Reihenfolge!)

```
smtpd_recipient_restrictions = permit_sasl_authenticated,
  permit_mynetworks,
  reject_non_fqdn_sender,
  reject_non_fqdn_recipient,
  reject_non_fqdn_hostname,
  reject_unknown_recipient_domain,
  reject_invalid_hostname,
  reject_unknown_hostname,
  reject_unknown_sender_domain,
  reject_rbl_client,
  permit_mx_backup,
  reject_unauth_destination
```

Das ganze nun Abspeichern und postfix wieder neu starten.
Wenn das ohne Fehler gelaufen ist, können wir nun an den Virenscanner gehen.

Holt euch von HBV http://www.antivir.de/download/download.htm den „AntiVir MailGate Linux“.
Für den Privaten Einsatz ist der kostenlos zu registrieren.
Entpackt ihn und ruf das install-script auf.

Nun müssen wir die main.cf von Postfix wieder anpassen:

```
unix:/etc/postfix/ # joe main.cf
```

sucht dort eine Zeile mit content_filter.
Falls sie nicht da ist, fügt sie hinzu. In jedem fall sollte das ganze dann so aussehen:

```
content_filter = smtp:127.0.0.1:10024
```

Das ganze nun Abspeichern, postfix noch nicht neu starten.
editiert nun die master.cf

```
unix:/etc/postfix/ # mcedit master.cf
```

Editiert dort die Zeile localhost so dass sie hinterher so aussieht:

```
localhost:10024 inet n - n      -       -     smtpd -o content_filter=
```

Das ganze nun Abspeichern und postfix neu starten.
Schaut wieder im Logfile, ob alles richtig läuft.
Wenn ja, dann schickt euch mal eine Mail.
Der Virenscanner sollte gleich loslegen (sichtbar mit tail –f /var/log/mail).

So. Das wars.

Mailserver

Eindeutige ID: #1000
Verfasser: Michael Stender
Letzte Änderung: 2008-03-01 20:29